INVESTIGATING AUTHENTICATION OF CHOICE USED BY SECURITY CRITICAL PROFESSIONALS IN HEALTH SETTING

Oluwadamilola Arinde, Jinjuan Feng and Ziying Tang
Towson University, Towson MD, USA

ABSTRACT

User authentication is a crucial security mechanism that plays an essential role in protecting systems and information. Numerous studies have examined users' experiences with various authentication methods. However, very few focused on granting users the freedom to select one or more authentication methods of their own choice. Limited research in this area suggested that the "Authentication of Choice" (AoC) approach can potentially serve as a usable and secure authentication solution on mobile devices. However, those studies only evaluated the AoC approach on the general population. No study examined the AoC approach as used by individuals in security-critical professions such as the military. To address this gap, we conducted an online longitudinal study with 12 military and 12 civilian participants to assess the AoC approach using a mobile app supporting healthy living. The result of the study provides insight into how users in special professions interact with and perceive the AoC approach in the context of mobile health apps.

KEYWORDS

Authentication of Choice, Usability, Security, Health Mobile App

1. INTRODUCTION

User authentication is a process employed to verify the identity claimed by a user before granting access to a system or an application. An effective user authentication method is crucial to prevent illicit access to any information service, especially health-related applications. Even though many studies have examined users' experiences with various authentication methods, very few studies have focused on the approach that grants users the freedom to select one or more authentication methods of their choice. Oluwafemi and Feng (2020) conducted studies to understand how users perceive the 'Authentication of Choice' (AoC) approach in the context of mobile applications. The results suggested that the AoC approach can serve as a usable and secure authentication solution on mobile devices. However, this work only evaluated the AoC approach on the Android platform when users executed tasks with low security and privacy concerns.

User perception about an authentication approach might differ when the nature of the tasks involves more sensitive information, such as those supported in health applications. We examine the impact of task and information sensitivity on the perception of AoC in the context of mobile health apps, and the results further confirm that users perceive multi-factor AoC as a usable and secure authentication method in the health setting (Arinde et al., 2022, pp. 228-240).

Users' perceptions may also differ depending on the nature of their profession. Users in the security-critical profession, such as the military, may have a different perspective towards authentication methods than the general public. In this paper, we report a study that aims to investigate the 'Authentication of Choice' approach used by individuals from special professions. With a split-plot design, the study assessed the performance and user perception of the AoC approach in the context of mobile health apps. 12 Military and 12 Civilian participants used three types of authentication processes: alphanumeric password, Single-Factor AoC, and Multi-Factor AoC, in 3 weeks. The results suggest the potential to adopt the authentication of choice approach in security-critical professions.

2. RELATED WORKS

2.1 Multiple Factor Authentication

In access control, validation is the initial phase. Usually, it employs authentication mechanisms categorized into three factors: something you know (knowledge factor), something you have (possession factor), and something you are (inherent factor) (Nilesh et al., 2016, pp. 246-249). An additional authentication factor is somewhere you are (location-based).

The traditional security procedure for user authentication is based on only one factor, called Single-Factor authentication (SFA) (Madhuravani et al., 2013, pp.1358-1361). The most popular SFA method is knowledge factor authentication, notably "passwords". The SFA is widely used but has several problems associated with it. Gunson et al (2011) made an argument in their study that despite the popularity of SFA methods, they are not strong enough to provide the needed level of security to the system. Numerous studies further supported this claim. (e.g., Dasgupta et al., 2016, pp. 85-116).

Multi-Factor Authentication (MFA) was subsequently proposed to provide a higher level of security by combining two or more distinct and different categories from the authentication factors (Abhishek et al., 2013). While multi-factor authentication improves the security of the authentication system, it may interfere with the usability of the system. One of the challenges is the user's lack of motivation (Das et al., 2018) because some users believe that multi-factor authentication is making the system more complex to use. Another study by Aleksandr et al (2018) classifies the usability challenges from three perspectives: task efficiency, task effectiveness, and user preference.

2.2 Authentication of Choice

To design a usable and secure system, Cranor and Buchler (2014) suggest that researchers need to go beyond using human-centered design techniques and adopt design techniques that give users the ability to make decisions. One of Ben Schneiderman's golden interface design rules, support of internal locus of control, addresses the user decision-making design approach concept. A sense of satisfaction comes with users knowing they are thought of during the design process and given the freedom to make choices in an application. Vance and Paik (2005) suggest user interface be designed so that users feel more responsible and accountable for their actions. If this is apparent in the interface, they will be less likely to misuse their access rights to the system.

As we have established that there is no perfect authentication method in terms of usability and security, this shows that no authentication method can accommodate all users. It will be challenging to design an authentication method that is universally accessible for users without the knowledge of their abilities and disabilities (Fairweather et al., 2002).

Users may also have a preferred authentication method depending on their physical abilities and cognitive skills (Belk et al., 2013, pp. 442-459). Hausawi et al (2014) proposed a choice-based authentication approach that can address the issues with current authentication methods, including security issues, usability issues, and universal access. According to the findings in (Oluwafemi and Feng, 2020; Arinde et al., 2022), the general users prefer the AoC method over the alphanumeric method. They also perceive the AoC method as easy to use, efficient, easy to remember, and secure.

2.3 Security and Usability of Mobile Health Applications

In the past decade, mobile health applications have grown exponentially due to their usefulness in telehealth, which requires remote patient monitoring. The pandemic further motivated the healthcare industry to integrate technology now more than ever for the benefit of all stakeholders ("Number of mHealth apps available in the Google Play Store," 2021).

The growth of mobile health apps has led to increasing challenges in protecting sensitive and personal data collected through those apps. Increasing vulnerabilities in the mobile health apps available have been widely reported. An assessment by Intertrust highlights significant security gaps in mHealth apps, one of them indicating that 71% of tested mHealth apps have a high-level security vulnerability ("Intertrust Releases 2020 Security Report on Global mHealth App Threats," 2020).

One of the high-level security vulnerabilities is the possibility of a data breach due to weak data encryption on the apps. Another one is 81% data leakage from COVID-tracking applications ("Intertrust Releases 2020 Security Report on Global mHealth App Threats," 2020).

With such security issues, it is understandable how the critical focus in developing mHealth apps is security. These applications' balance of security and usability is crucial for successful adoption and high-quality service.

2.4 User Authentication in Special Professions

The operations of many special professions, such as the military, first responders, and healthcare, require substantially higher security and privacy practice than the other fields. With the sensitive nature of the military, user authentication is a crucial part of its operations. Military personnel must gain access to applications using an authentication method. According to login.gov ("Authentication Options," 2023), military personnel must set up multi-factor authentication as an added layer of protection to secure information. They offer their personnel multiple authentication options, with Security Keys, PIV/CAC cards, and authentication apps being considered the most secure options ("Authentication Options," 2023).

Although the military favors Security keys and PIV/CAC, these physical objects can be misplaced, lost, or stolen. Authentication apps such as Google Authenticator are great options for the general public as they are mobile applications that can be downloaded on the phone to generate a one-time password and are considered secure. However, they may cause security implications in the military setting. Finding the balance between the security and usability provided by various options can improve military personnel's' perception of user authentication.

The longitudinal study reported in the following sections is the first study that investigated the use of Authentication of Choice in healthcare by military professionals.

3. METHODS

3.1 Study Goal

This online longitudinal study aims to examine the performance and user perception of the Authentication of Choice approach by military professionals in the context of mobile health-related applications. The study adopted a split-plot design with two participant groups (military and civilian) and three conditions for authentication:

- Alphanumeric Password: Participants signed up and logged in with email and password.
- Single-Factor AoC: Participants chose one authentication method out of five options (alphanumeric passwords, pin, phone's One Time Password (OTP), face recognition, and fingerprint authentication).
- Multi-Factor AoC: Participants chose two authentication methods from the five options listed above.

3.2 Participants

Twenty-four participants took part in the study. Twelve of the participants are members of the Military, while the other twelve are civilian participants. All the participants are between the ages of 22 – 43 years. There were nine males and three females from each group. Sixteen participants used iPhones, and eight used Android phones. Nineteen of the participants have a bachelor's degree or higher. The military participants work in various specialties such as Machinery, Intelligence, and healthcare. The civilian participants also work in various fields, such as IT, healthcare, and engineering. No financial incentive was provided for participating in the study.

3.3 HealthyCog Application

An application named "HealthyCog" was developed for this study. The application is a cross-platform application that can be used on both iOS and Android platforms. The app presents five authentication methods that are commonly adopted in commercial mobile devices:

- Alphanumeric email and password
- Personal Identification Number (PIN)
- One-Time-Password (OTP) via SMS
- Face Recognition
- Fingerprint Recognition

The application design followed general usability guidelines and underwent several rounds of testing based on user feedback. Users will create and test a different type of authentication condition each week:

- Type 1: Alphanumeric email and password
- Type 2: Single-Factor authentication of choice with five options
- Type 3: Multi-Factor authentication of choice (Two) with five options

Figure 1 below shows the user interface of the HealthyCog app featuring the home page where users can sign up or login. The sign-up button leads to the registration page where participants will select the account type to test for the week.

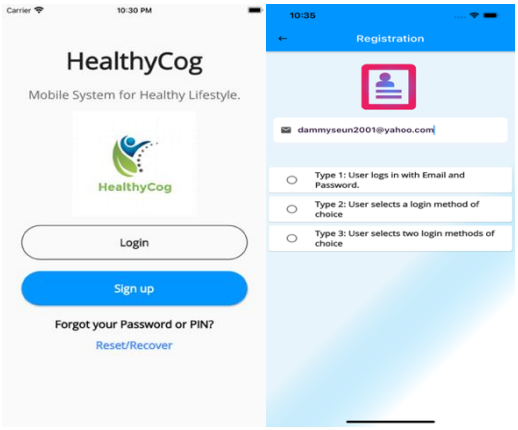

Figure 1. Home page and registration page of the HealthyCog app

4. PROCEDURE

The study was conducted online. After providing consent to participate in the study, Instructions about the study environment and procedure were emailed to participants. A demographic questionnaire was completed at the beginning of the study. Each participant used the app for three weeks, interacting with one authentication condition each week. The order of the three authentication conditions was counterbalanced among the participants to control the learning effect.

During the study, participants first installed the 'HealthyCog' app from the App Store or Google Play Store, depending on if they had an iOS or an Android phone. Following successful installation, each participant created an account on the app. The type of account created depended on the order in the instructions they received. The participants then logged into the account daily for the next seven days. After logging in, they completed one of the following health-related tasks:

– Select the 'HealthyCog Chatbot' function and schedule a tentative appointment (This is a fictional task; no actual appointment is made)

– In the 'HealthyCog Arm' function, watch an arm exercise video and, if interested, perform the arm exercise

– In the 'Med Reminder' function, add a fictional medication, set a reminder, and select a time interval for the reminder

– Visit the 'Daily Steps' function to activate the pedometer and walk for a few minutes if possible. The number of steps taken is displayed at the end of the exercise.

At the end of the first week, participants completed a questionnaire about the session via Google Forms before switching to the following account type specified in the instruction. After completing all three sessions,

participants completed a post-study questionnaire where they rated their preference for each of the three authentication processes.

The app automatically logged the sign-up and log-in time for the three conditions and the authentication methods chosen during the single-factor and multi-factor Authentication of Choice processes into a secure database.

5. RESULTS

5.2 Average Login Time

A split-plot Analysis of the Variance test with login time as the dependent variable and profession and type of authentication as the independent variables suggests no significant difference in login time between the military and civilian groups ($F(1, 22) = 0.438$, n.s.). There is a significant difference in login time between the three authentication conditions ($F(2, 44) = 12{,}21$, $p < 0.001$). Figure 2 shows the average login time of the three conditions in seconds per group. Participants spent a shorter time signing into an account in the single-factor AoC condition than in the other two conditions.

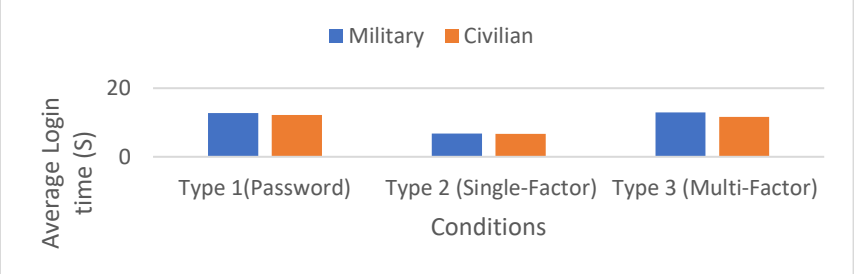

Figure 2. Average login time of the three conditions in seconds per group

5.3 Authentication Method chosen for AoC

Table 1 and Table 2 illustrate the number and percentage of military and civilian participants who chose each authentication method under the single-factor AoC and multi-factor AoC conditions. In the multi-factor AoC condition, each participant chose two methods. Therefore, the total number of participants choosing all methods is 24, and the total percentage of participants is 200% for each table.

Table 1. Number and percentages of military participants who chose each method under Type 2 and Type 3 conditions

Authentication Method	Type 2	Type 3	Type 2%	Type 3%
Password	1	2	8.3%	16.7%
Pin	5	10	41.7%	83.3%
OTP	1	6	8.3%	50%
Fingerprint	2	2	16.7%	16.7%
Face Recognition	3	4	25%	33.3%
Total	12	24	100%	200%

As illustrated in Table 1, the PIN authentication method is the most frequently chosen in both conditions at 41.7% and 83.3%, respectively. For single-factor AoC, the second most frequently chosen method was Face Recognition at 25%, and Fingerprint came third at 16.7%. The SMS OTP and the Password methods were the least chosen by 1 participant each. Similar results in the ranking were observed for multi-factor AoC for the PIN method. The OTP was the second most frequently chosen method, Face Recognition as the third, while Fingerprint and Password tied as the fourth.

Table 2. Number and percentages of civilian participants who chose each method under Type 2 and Type 3 conditions

Authentication Method	Type 2	Type 3	Type 2%	Type 3%
Password	0	3	0%	25%
Pin	3	9	25%	75%
OTP	2	6	16.7%	50%
Fingerprint	2	1	16.7%	8.3%
Face Recognition	5	5	41.6%	41.7%
Total	12	24	100%	200%

As shown in Table 2, for the civilian group, the most frequently chosen method for single-factor AoC was Face Recognition at 41.6%, the Pin method came second at 25%, while Fingerprint and OTP tied as third at 16.7% each. The Password method was not chosen in this method of AoC. For multi-factor AoC, the PIN method was the most frequently chosen, while OTP was the second. Face Recognition was the third. The Password method was selected by 3 participants making it the fourth and fingerprint the least chosen. Figures 3 and 4 show the percentages of participants who chose each method under the single-factor AoC and the multi-factor AoC conditions, respectively.

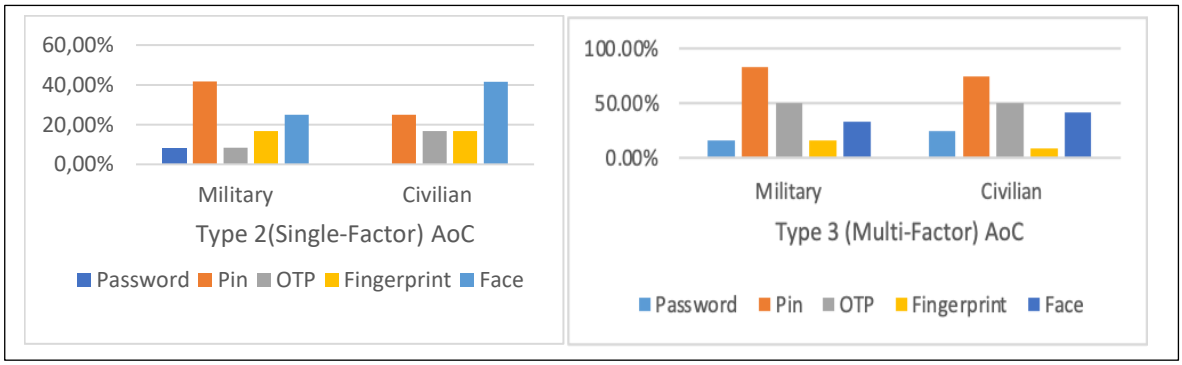

Figure 3. Percentages of participants who chose each method under Type 2 condition per group

Figure 4. Percentages of participants who chose each method under Type 3 condition per group

5.4 Preferred Authentication Process

In the post-study questionnaire, we asked the participants to rank their preferences towards the three authentication processes based on all factors combined. Tables 3 and 4 illustrate how the participants ranked each process for each group.

Table 3. Number and percentages of military participants who ranked each of the three conditions as their first, second, and third choice

Rank	Alphanumeric Password number (%)	Single-Factor number (%)	Multi-Factor number (%)	Total
First	0 (0%)	4 (33.3%)	8 (66.7%)	12
Second	2 (16.7%)	7 (58.3%)	3 (25)	12
Third	10 (83.3%)	1 (8.3%)	1 (8.3%)	12
Total	12	12	12	

We can see from Table 3 above 66.7% of the Military participants ranked the multi-factor AoC as their first choice. 33.3% chose the single-factor AoC as their first choice. No one chose the alphanumeric password condition. For the second choice, 58.3% chose the single-factor AoC as their second choice, 25% selected multi-factor AoC as their second choice, and 16.7% selected alphanumeric as their second choice. The least preferred process of the three is the alphanumeric password at 83.3%, while multi-factor and single-factor tie at 8.3%.

Table 4. Number and percentages of civilian participants who ranked each of the three conditions as their first, second, and third choice

Rank	Alphanumeric Password number (%)	Single-Factor number (%)	Multi-Factor number (%)	Total
First	0 (0%)	6 (50%)	6 (50%)	12
Second	1 (8.3%)	6 (50%)	5 (41.7)	12
Third	11 (92.7%)	0 (0%)	1 (8.3%)	12
Total	12	12	12	

Table 4 shows that the Civilian participants ranked the single-factor and multi-factor AoCs as their first choice at 50% each. None of them selected the alphanumeric method. For the second choice, 50% chose the single-factor AoC as their second choice, 41.7% selected multi-factor AoC as their second choice, and 8.3% selected Alphanumeric as their second choice. The least preferred process of the three is also the alphanumeric password at 92.7%, multi-factor was selected as the least preferred by 1 participant, and none selected the single-factor as their least preferred.

5.5 Perception of Usability and Security

In the post-study questionnaire, participants were asked to rank their satisfaction with the security, speed, memorability, and ease of use of each authentication approach using a Likert scale of five points (5- strongly agree, 1 – strongly disagree). All the military group and 92% of the civilian group strongly agreed that the multi-factor AoC improved security. No participant from the military group agreed that the multi-factor AoC took too long. One participant from the civilian group strongly agreed that AoC took too much time. No participant from the military group and only one participant from the civilian group agreed that the multi-factor AoC was challenging to remember. Finally, no participant from the military group agreed that the multi-factor AoC was difficult to use. Only one participant from the civilian group strongly agreed.

When asked for their preferred choice regarding ease of use, both groups of participants ranked single-factor authentication as their first choice (100%). When asked for their preference on the most secured, 100% of the participants in both groups chose the multi-factor AoC as their first choice.

Overall, all military participants have highly positive perceptions regarding both usability and security towards the multi-factor AoC process and are likely to adopt the approach. The perception of the civilian group towards the multi-factor AoC is also positive.

6. DISCUSSION AND LIMITATIONS

We conducted the first study that investigated the use of Authentication of Choice in the healthcare context by professionals from the military. The results suggested that for all factors combined, the multi-factor Authentication of Choice is the most preferred approach by the military participants, with single-factor authentication as the second and the Alphanumeric password the lowest. For civilians, the single-factor and multi-factor AoC approaches were ranked similarly overall, while the alphanumeric approach was the least preferred. Both the military and the civilian participants' preference towards the multi-factor authentication of choice approach over the alphanumeric password suggests that participants like the freedom of choosing authentication methods during authentication. The military group's preference towards the multi-factor AoC approach over the single-factor AoC approach could be attributed to the extra layer of security that multi-factor authentication provides.

Regarding specific measures, both groups of participants perceived the single-factor Authentication of Choice as the most preferred in terms of ease of use and the multi-factor authentication as the most preferred in terms of security. Overall, the results confirmed the potential to adopt the authentication of choice approach by critical security professionals. They also further validated the findings of previous studies (Oluwafemi and Feng, 2020; Arinde et al., 2022) on the adoption of AoC in general and health-related mobile applications to improve user experience and security.

Regarding limitations, the study only investigated a limited set of authentication methods. Some commonly adopted techniques, such as gesture passwords and location-based authentication were not examined. In addition, the number of participants is fairly small and may not represent the diverse user characteristics of the general public or the military profession. We plan to include a broader set of authentication methods and larger, more diverse participants in future studies.

REFERENCES

Abhishek, S. et al., 2013. A Comprehensive Study on Multifactor Authentication Schemes, Meghanathan, N. et al., Advances in Computing and Information Technology. Vol. 177. Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-31552-7_57.

Aleksandr, O. et al., 2018. Multi-Factor Authentication, A Survey. *Cryptography*, Vol. 2, issue 1, doi:10.3390/cryptography2010001.

Arinde, O. et al., 2022. A Preliminary Investigation of Authentication of Choice in Health-Related Mobile Applications. *Proceedings of 24th HCII.* Pp. 228-240.

Authentication options | Login.gov. www.login.gov. Retrieved April 18, 2023, from https://www.login.gov/help/get-started/authentication-options.

Belk, M. et al., 2013. Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms. *Proceedings of the IFIP TC13 Conference on Human-Computer Interaction*. South Africa, pp. 442-459. 2013.

Cranor, L. and Buchler, N., 2014. Better Together: Usability and Security Go Hand in Hand. *In IEEE Security & Privacy*, vol. 12, no. 6, pp. 89-93, doi: 10.1109/MSP.2014.109.

Das, S. et al., 2018. Why Johnny Doesn't Use Two Factor a Two-Phase Usability Study of the FIDO U2F Security Key. *In International Conference on Financial Cryptography and Data Security (FC)*.

Dasgupta, D. et al., 2016. Toward the design of adaptive selection strategies for multi-factor authentication. *Computers & Security*. Vol. 63, pp. 85-116, 2016, doi: 10.1016/j.cose.2016.09.004.

Fairweather, P. et al., 2002. From assistive technology to a web accessibility service. *In International Conference on Assistive Technologies (ASSETS). ACM*.

Gunson, N. et al., 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*. Vol. 30, no. 4, pp. 208–220, doi: 10.1016/j.cose.2010.12.001.

Hausawi, Y. et al., 2014. Choice-Based Authentication: A Usable-Security Approach, Stephanidis, C. et al., Universal Access in Human-Computer Interaction. Design and Development Methods for Universal Access. *In UAHCI Lecture Notes in Computer Science*. Vol. 8513, Springer, Cham. https://doi.org/10.1007/978-3-319-07437-5_12.

Madhuravani, B. et al., 2013. A Comprehensive Study on Different Authentication Factors. *IJERT*. Vol. 2, no. 10, pp. 1358-1361.

Nilesh, A. et al., 2016. A Review of Authentication Methods. *IJSTR*. Vol. 5, no. 11, pp. 246-249, 2016.

Number of mHealth apps available in the Google Play Store from 1st quarter 2015 to 1st quarter 2021. Statista https://www.statista.com/statistics/779919/health-apps-available-google-play-worldwide/, last accessed 2021/12/17.

Oluwafemi, J. and Feng, J., 2020. How Users Perceive Authentication of Choice on Mobile Devices. *Proceedings of 13th International Conference on Advances in Computer-Human Interactions*. Pp. 345-351.

Vance, C. and Paik, Y., 2005. Forms of Host-Country National Learning for Enhanced MNC Absorptive Capacity. *Journal of Managerial Psychology*. Vol. 20, no. 7, pp. 590–606.

Intertrust Releases 2020 Security Report on Global mHealth App Threats. www.businesswire.com. https://www.businesswire.com/news/home/20200929005146/en/Intertrust-Releases-2020-Security-Report-on-Global-mHealth-App-Threats#:~:text=Intertrust%20released%20their%202020%20Security,a%20breach%20of%20medical%20data.last accessed 2022/02/17.